SOC FORUM 2023

Управление аналитиками: инструкция по выживанию

SOC
FORUM
2023

Ратникова Анна

Руководитель группы мониторинга
Инфосистемы Джет

В чем уникальность аналитика SOC?

SOC как место встречи разных направлений

SOC FORUM 2023

ПРЕСЕЙЛ МЕНЕДЖЕР

Производит оценку оказания услуги

МЕНЕДЖЕР ПРОЕКТА

Ведет краткосрочный проект для оказания услуги

СЕРВИСНЫЙ МЕНЕДЖЕР

Ведет непрерывный контракт для оказания услуги

ИНЖЕНЕРЫ

Производят внедрение или поддержку эксплуатации продукта

АНАЛИТИКИ

Производят мониторинг и проводят углубленные расследования инцидентов в инфраструктуре заказчика

Подход к работе

SOC FORUM 2023

При решении задачи у инженера и аналитика абсолютно разный набор данных, с которыми можно работать

ИНЖЕНЕРЫ

Линейный подход

- Инструкция
- Вендор
- Инструмент
- Коллега, который решал похожий кейс

АНАЛИТИК

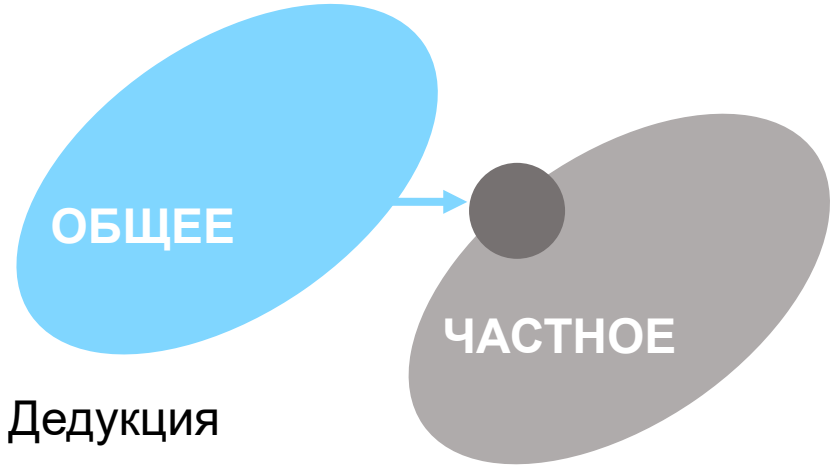
Параллельный подход

- Дата и время
- Узел
- Перезагруженный узел или ненастроенный аудит

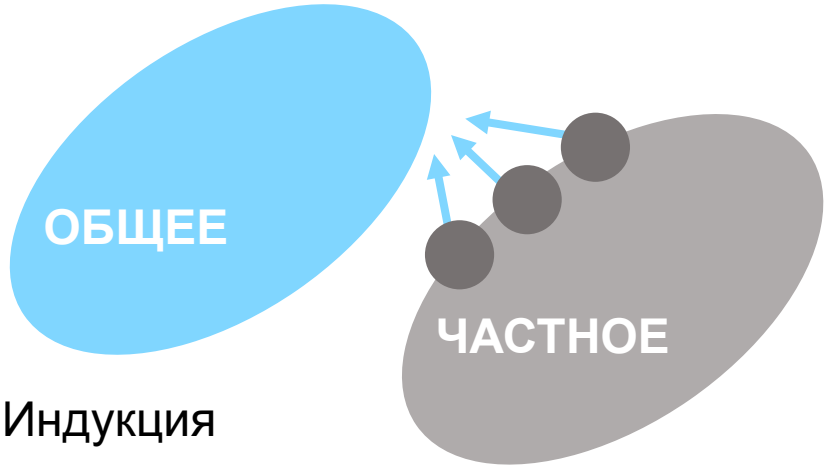
Ключ к пониманию

SOC FORUM 2023

Руководителю важно понимать ход выстраивания рабочего процесса для создания команды



Дедукция



Индукция

Выбор аналитика

SOC FORUM 2023

На какие качества нужно обратить внимание при поиске аналитика?

- Базовые разносторонние знания
- Целеустремленность
- Анализ
- Их мало ☹
- Постоянное изучение нового
- Усидчивость
- Грамотная структурированная речь

Взгляд с другой стороны

SOC FORUM 2023

Буквально 99% собеседований
на аналитика SOC

Они думают, что знают
и умеют все, пока
не сталкиваются
с реальностью работы
в интеграторе

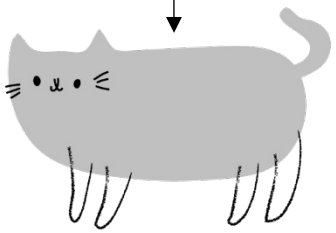
SOC FORUM 2023

Аналитики, которые выросли из первой линии, обычно очень любят и горят работой, но если спросить о будущем, то скорее всего не будут знать как им быть и что им делать

аналитика-джуна SOC

Жизненный цикл любого кота

любознательный и заряженный новичок



изучивший процессы и особенности работы

заскриптованный и растерявший базу

знает базу, но не умеет работать

SOC FORUM 2023

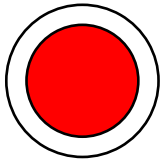
Задачи аналитика SOC

Выбор направления

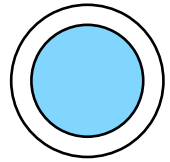
SOC FORUM 2023

В какой-то момент базы становится достаточно и аналитики буквально хотят попробовать все

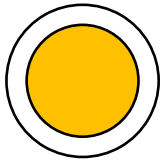
Какую кнопку нажмешь ты?



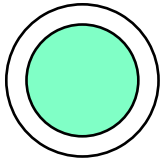
Red
Любишь поагрессивнее?



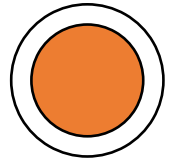
Blue
Ахаха, а нет,
Ты сейчас тут



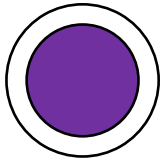
Yellow
О, багбаунти



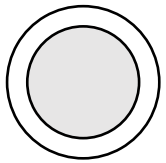
Green
Жду принт RnD



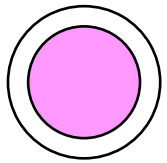
Orange
Найду акк бывшей
по маникюру



Purple
И такая команда
уже есть



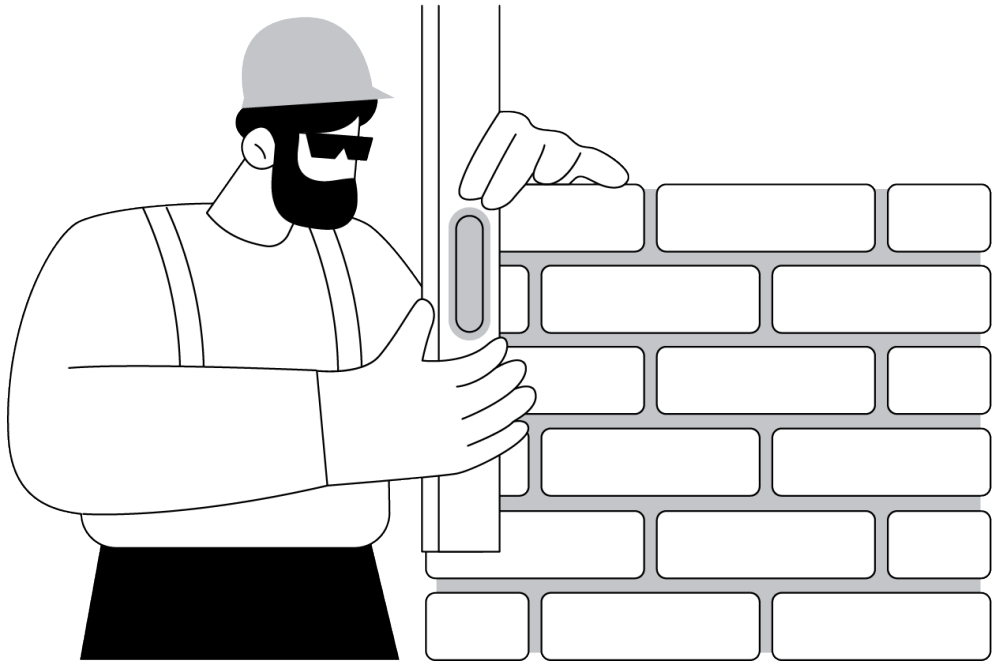
Grey
В суде поговорим



Pink
Тот самый,
кто смог в реверс

Выбор любой кнопки

SOC FORUM 2023



ожидание

реальность

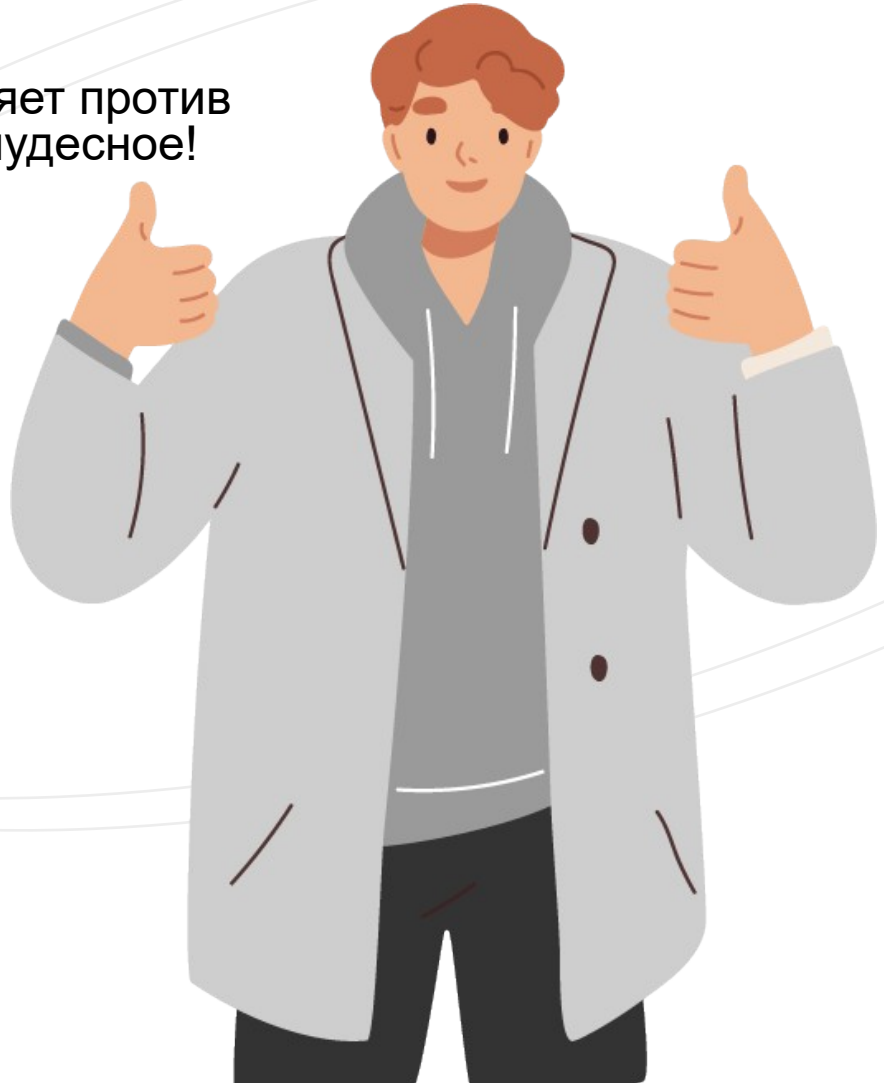
В итоге получаем его!

SOC FORUM 2023

ПАРАНОИК ОПТИМИСТ

Мир замышляет против меня что-то чудесное!

За мной по пятам следует счастье!



Меня всюду преследует удача

За каждым углом меня подстерегает успех

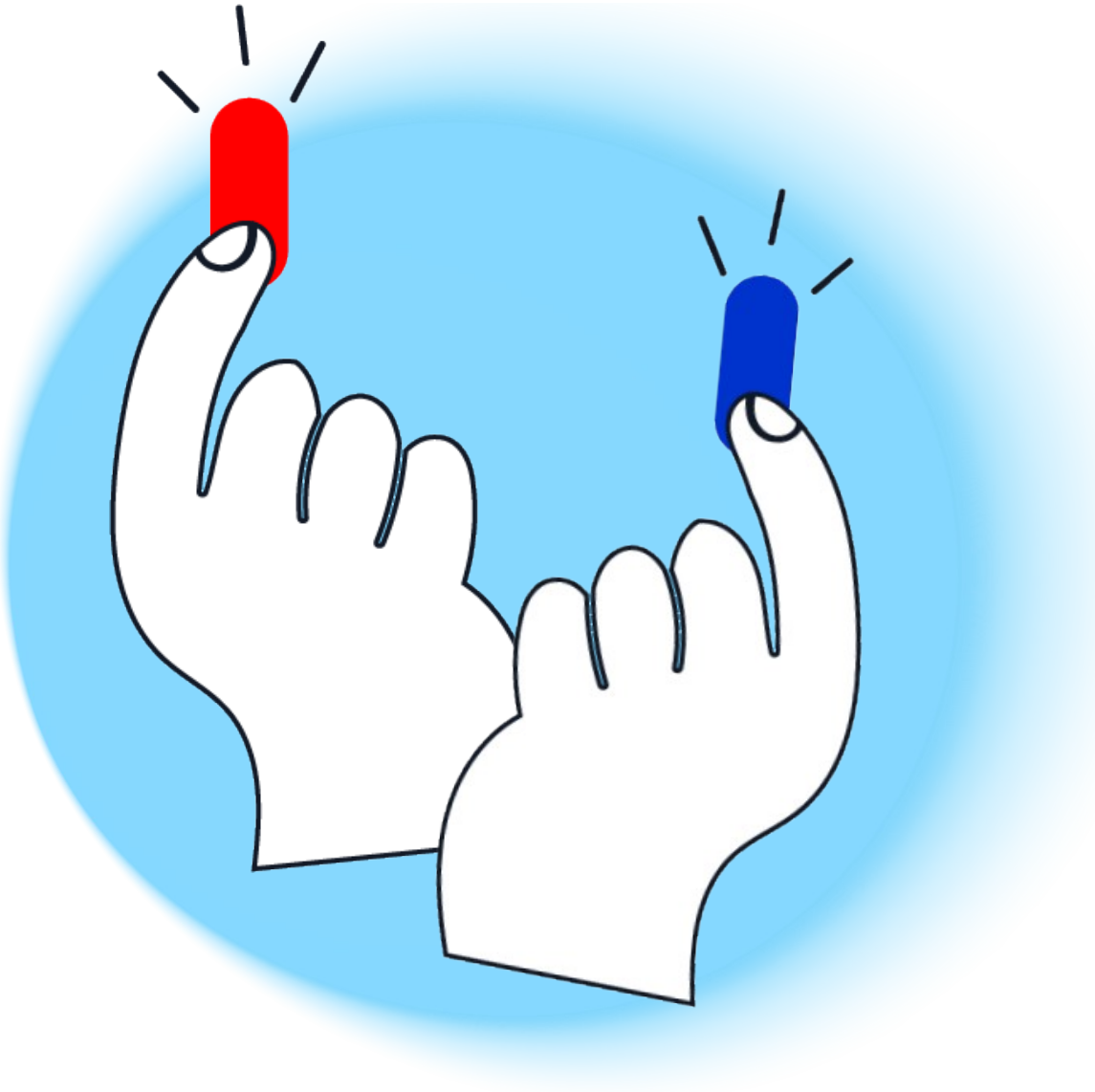
Меня собирается похитить любовь

Как повысить качество?

- Направление
- Доверяйте новичкам
- Параллельный анализ
- Избегаем граблей
- Разрабатываем роли, учимся делегированию
- Анализ проблем
- Поддержка
- Работа со сложными кейсами в парах

А что делать с балансом?

SOC FORUM 2023



- Приоритет
- Осознанность сотрудника
- Привлечение ресурсов

SOC FORUM 2023

Как не потерять любовь к работе?

Бережно и с любовью

- Баланс в работе
- Поддержка
- Кураторство

Новые задачи:

- Обучения
- Новые направления
- Challenge

SOC FORUM 2023

Аналитика – это по любви

СПАСИБО ЗА ВНИМАНИЕ!

Ратникова Анна

Руководитель группы мониторинга
Инфосистемы Джет

SOC FORUM 2023